

**UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF OKLAHOMA**

**KATHY DEEVERS, individually and on behalf
of all others similarly situated,
and
VENELIN STOICHEV, individually and on
behalf of all others similarly situated,**

Plaintiffs,

v.

WING FINANCIAL SERVICES, LLC,

Defendant.

**Case No. 22-CV-0550-CVE-JFJ
BASE FILE
(Consolidated with
Case No. 23-CV-0026-CVE-JFJ)**

OPINION AND ORDER

Before the Court are defendant's motion to dismiss (Dkt. # 25); plaintiffs' response (Dkt. # 29); and defendant's reply (Dkt. # 31). This putative class action suit, brought by representative plaintiffs Kathy Deevers and Venelin Stoichev, arises out of a data breach of Wing Financial Services, LLC ("Wing") servers. On March 1, 2023, this Court consolidated plaintiff Deevers' suit, filed December 19, 2022, with plaintiff Stoichev's suit, filed January 17, 2023. Plaintiffs jointly filed an amended complaint on March 17, 2023, alleging claims of negligence (count 1), negligence per se (count 2), breach of fiduciary duty (count 3), unjust enrichment (count 4), breach of implied contract (count 5), and violation of the Oklahoma Consumer Protection Act (count 6). On May 8, 2023, defendant moved, pursuant to Fed. R. Civ. P. 12(b)(1) and (6), to dismiss plaintiffs' claims (Dkt. # 25).

I.

Wing is an independently owned and operated Jackson Hewitt franchise that provides financial and tax-preparation services. Dkt. # 21, at 2. Representative plaintiffs, along with the

putative class members, are clients and “consumers” of Wing. Id. at 8. In order to provide financial services, Wing acquires personal and financial information from its clients and consumers. Id. at 2.

On August 7, 2022, Wing discovered that its network servers were exposed in a data breach, resulting in access to “highly sensitive” client records by unauthorized third-parties. Id. at 2, 12. This data breach, affecting 243,403 people, resulted in the exposure of personally identifiable information (“PII”). Id. at 2. Client information at risk included “name[s], Social Security number[s], medical data, insurance information, government identification, state identification, driver’s license number[s], financial account number[s] and access code[s], tax identification number[s], address[es], biometric information, birthday[s], health insurance and policy information, and payment card number[s].” Id. at 13. Plaintiffs were not aware of the breach until December 1, 2022, when Wing sent a letter to clients notifying them of the breach and providing a complimentary year subscription for credit monitoring and identity protection.¹ See Dkt. 34-1, at 4.

In its letter, Wing “confirmed these records relate[d] to one Wing [] server.” Id. at 5. Wing briefly outlined steps it had taken to rectify the breach, including “immediately limit[ing] access to

¹ When a defendant, in a motion to dismiss under Rule 12(b)(1), facially attacks a complaint on its sufficiency of claims and not their truthfulness, the court must accept the plaintiffs’ allegations as true. Pueblo of Jemez v. U.S., 790 F.3d 1143, 1148 n.4 (10th Cir. 2015). Courts, however, may “consider not only the complaint itself, but also attached exhibits, and documents incorporated into the complaint by reference” when evaluating a motion to dismiss. Smith v. United States, 561 F.3d 1090, 1098 (10th Cir. 2009). In one hyperlinked footnote in the amended complaint, see Dkt. # 21, at 13 n.8, plaintiffs presented two documents: a public notice sent by Wing to the Attorney General of Maine on December 1, 2022, and a notice sent to clients on that same date regarding the security breach. Because, pursuant to LGnR2-5, hyperlinks are permissible only for “links to legal references and citations,” the Court directed plaintiffs to file the referenced documents as a separate exhibit, which was filed at Dkt. # 34-1. Because plaintiffs refer to these documents throughout the complaint, the Court may consider them as an attached exhibit. See Smith, 561 F.3d at 1098.

the potentially affected servers,” “chang[ing] all of its user’s login credentials,” and “further train[ing] its employees on securing information.” Id. Wing also offered information about complimentary credit monitoring, placing fraud alerts, freezing credit files, and reporting identity fraud to the IRS. Id. at 5–10. In a formal notice to the Maine Attorney General, Wing wrote that, after learning of the breach on August 7, 2022, it launched an internal investigation and hired independent experts to ascertain the extent of the breach. Id. at 3. After confirming that the breach had exposed personal client information, Wing notified clients and undertook the aforementioned security measures. Id. at 2.

Plaintiffs allege that Wing failed to implement reasonable data security measures to protect its client information. Dkt. # 21, at 3. They contend that Wing carelessly maintained files and failed to properly encrypt client data. Id. at 3, 9, 21. According to plaintiffs, Wing could have prevented the data breach entirely had they employed security measures consistent with the industry standard. Id. at 10–11, 21. Plaintiffs also state that they remain “in the dark about what particular data was stolen, the particular malware used, and what steps are being taken . . . to secure” their personal information. Id. at 14.

As a result of the breach, plaintiffs maintain that they have suffered or will suffer “actual identity theft, including fraudulent credit inquiries and cards being opened in their names.” Id. at 22. They allege that their PII was improperly disclosed and they are at an increased and imminent risk of identity theft for which they are entitled compensation. Id. Representative plaintiffs claim they have or will suffer fear and anxiety as a result of this risk. Id. Plaintiffs also maintain that they will likely lose access to their credit and bank accounts, and will face an increased cost of borrowing

as a result of their potentially reduced credit score. Id. Plaintiffs do not allege that these purported harms have yet occurred.

Plaintiffs further assert that this breach amounted to “trespass, damage to, and theft of their personal property,” and culminated in the “loss of [their] privacy.” Id. They claim ascertainable losses “in the form of deprivation of the value of [their] personal [and health] information for which there is a well-established and quantifiable national and international market” and “value of their time reasonably expended to remedy or mitigate the effects of the [d]ata [b]reach.” Id. Plaintiffs and purported class members conclude they also have an interest in ensuring their PII is safeguarded against further exposure. Id.

Representative plaintiffs allege additional harms. Deevers, a resident of Oklahoma, asserts that she had “previously received tax preparation services” as a client of Wing. Id. at 6. She alleges that she has expended and will continue to expend considerable time and money monitoring her accounts for fraud, and claims to suffer “fear and anxiety” due to this allegedly heightened risk of identity theft. Id. at 7.

Stoichev, another resident of Oklahoma and “consumer” of Wing, asserts that his data was among that accessed in the breach. Id. at 4. Beyond the diminution in the value of his personal information, lost time, anxiety, and inconvenience, plaintiff claims he was notified “that a person in another state . . . attempted to make a purchase using his Best Buy Visa gift card.” Id. at 4, 6. However, plaintiff has not asserted that he provided the Best Buy Visa gift card information to Wing in the course of obtaining financial services. Best Buy verified that the person attempting to use plaintiff’s card was not Stoichev, and refused to authorize the purchase. Id. Plaintiff alleges he has also received an increase in spam calls from loan companies. Id.

II.

Motions to dismiss under Rule 12(b)(1) “generally take one of two forms. The moving party may (1) facially attack the complaint’s allegations as to the existence of subject matter jurisdiction, or (2) go beyond allegations contained in the complaint by presenting evidence to challenge the factual basis upon which subject matter jurisdiction rests.” Merrill Lynch Bus. Fin. Servs., Inc. v. Nudell, 363 F.3d 1072, 1074 (10th Cir. 2004) (internal citation and quotations omitted). Where a motion to dismiss is based on a facial attack, as here, courts “apply the same standards under Rule 12(b)(1) that are applicable to a Rule 12(b)(6) motion to dismiss for failure to state a cause of action.” Muscogee (Creek) Nation v. Okla. Tax Comm’n, 611 F.3d 1222, 1227 n.1 (10th Cir. 2010).

In considering a motion to dismiss under Fed. R. Civ. P. 12(b)(6), a court must determine whether the claimant has stated a claim upon which relief may be granted. A motion to dismiss is properly granted when a complaint provides no “more than labels and conclusions, and a formulaic recitation of the elements of a cause of action.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 (2007). A complaint must contain enough “facts to state a claim to relief that is plausible on its face” and the factual allegations “must be enough to raise a right to relief above the speculative level.” Id. (citations omitted). “Once a claim has been stated adequately, it may be supported by showing any set of facts consistent with the allegations in the complaint.” Id. at 562. Although decided within an antitrust context, Twombly “expounded the pleading standard for all civil actions.” Ashcroft v. Iqbal, 556 U.S. 662, 683 (2009). For the purpose of making the dismissal determination, a court must accept all the well-pleaded allegations of the complaint as true, even if doubtful in fact, and must construe the allegations in the light most favorable to a claimant. Twombly, 550 U.S. at 555; Alvarado v. KOB-TV, L.L.C., 493 F.3d 1210, 1215 (10th Cir. 2007); Moffett v. Halliburton

Energy Servs., Inc., 291 F.3d 1227, 1231 (10th Cir. 2002). However, a court need not accept as true those allegations that are conclusory in nature. Erikson v. Pawnee Cnty. Bd. of Cnty. Comm’rs, 263 F.3d 1151, 1154–55 (10th Cir. 2001). “[C]onclusory allegations without supporting factual averments are insufficient to state a claim upon which relief can be based.” Hall v. Bellmon, 935 F.2d 1106, 1109–10 (10th Cir. 1991).

III.

Defendant argues that, under Rule 12(b)(1), the Court lacks subject-matter jurisdiction because plaintiffs have not suffered an injury in fact as required to establish standing under Article III. Dkt. # 25, at 9. Defendant asserts that “[w]hile [p]laintiffs allege that third-party malicious actors accessed their information during an intrusion” into Wing servers, “they do not allege facts showing that their information was removed and then actually misused.” Id. “Without actual misuse,” according to defendants, “any alleged harm fails to satisfy Article III because it is a self-created harm based on speculative future injury that may never come into fruition.” Id. Plaintiffs respond that they allege many harms, “including expending a significant amount of time dealing with [the data breach’s] fallout, diminished value of their personal data, . . . an attempted fraudulent credit card transaction, and marked increase in phone calls from loan companies.” Dkt. # 29, at 9. Plaintiffs assert that, regardless, actual fraud or misuse is not required to establish an injury in fact sufficient for standing purposes. Id. at 10. Defendant contends that these latter allegations—even if sufficient to show a concrete and imminent injury in fact—are not fairly traceable to the defendant’s conduct. Dkt. # 25, at 17, 19–20.

Article III of the United States Constitution limits federal courts to resolve only “cases” or “controversies.” U.S. Const. art. III, § 2. “For there to be a case or controversy under Article III, the

plaintiff must have a personal stake in the case—in other words, standing.” TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2203 (2021) (internal quotations omitted). “The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing” standing. Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016). To establish standing, plaintiffs must allege that (1) they suffered an injury in fact, that is (2) fairly traceable to the defendant’s conduct and (3) redressable by the court, for each discrete claim that they advance. Lujan v. Defs of Wildlife, 504 U.S. 555, 560–61 (1992). In a putative class action, representative plaintiffs are further required to show that “they personally have been injured,” not just “that injury has been suffered by other, unidentified members of the class to which they belong.” Spokeo, 578 U.S. at 338 n.6 (citing Simon v. Eastern Ky. Welfare Rights Org., 426 U.S. 26, 40 n.20 (1976)) (internal quotations omitted).

An injury in fact must be “concrete, particularized, and actual or imminent.” TransUnion, 141 S. Ct. at 2203. Each of these components is independently necessary to establish injury in fact—it is not enough, for example, that an alleged injury is individualized, or particular, to the plaintiff—that injury must also be concrete, or “real rather than abstract.” Laufer v. Looper, 22 F.4th 871, 876 (10th Cir. 2022) (internal quotations omitted); see Spokeo, 578 U.S. at 340. Similarly, that concrete and particularized harm must be actual (i.e., actively occurring or already occurred) or imminent (i.e., certainly impending). Lujan, 504 U.S. at 560; Clapper v. Amnesty Int’l USA, 568 U.S. 398, 409 (2013).

Harms need not be tangible, i.e., cause physical or monetary harm to the plaintiff, to suffice for concreteness. See TransUnion, 141 S. Ct. at 2204. Various intangible harms such as the “disclosure of private information” or “intrusion upon seclusion” can be concrete because they bear a close relationship “to harms traditionally recognized as providing a basis for lawsuits in American

courts.” Id. In the data breach context, actual identity theft and fraud are sufficiently concrete injuries; however, “in a suit premised on the *mere risk*” of future identity theft or fraud, courts “must also consider the type of relief sought” by the plaintiff. Clemens v. ExecuPharm Inc., 48 F.4th 146, 155 (3d Cir. 2022) (emphasis added). In the wake of TransUnion, a plaintiff suing for damages must allege that the data breach “caused additional, currently felt concrete harms” on top of alleging an imminent risk of future harm. Clemens, 48 F.4th at 155–56; see also Lupia v. Medicredit, Inc., 8 F.4th 1184, 1193 n.3 (10th Cir. 2021) (“we recognize the difficulties in bringing a claim for damages based on a theory of future risk of harm”); Dinerstein v. Google, LLC, 73 F.4th 502, 512 (7th Cir. 2023) (“while an imminent risk of future harm may suffice to support standing to sue for prospective relief (i.e., an injunction), a claim for damages requires a concrete harm that has in fact occurred”). When seeking injunctive relief, however, plaintiffs need only plead that the risk of future identity theft or fraud is sufficiently “imminent” as required under Article III. See Legg v. Leaders Life Ins. Co., 574 F. Supp. 3d 985, 992–93 (W.D. Okla. 2021).

Alleged future harms must be “certainly impending” or at a “substantial risk . . . [to] occur” to suffice as imminent for Article III standing. Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014). “Allegations of *possible* future injury do not establish an injury in fact.” Doe by & through Doe v. Hunter, 796 F. App'x 532, 536 (10th Cir. 2019) (emphasis added).² The importance of establishing imminence is plainly apparent in the context of data breach litigation. Imminence “ensure[s] that [an] alleged injury is not too speculative.” Clapper, 568 U.S. at 409. When a concrete harm from a data breach has yet to actualize, standing cannot be predicated on a speculative

² Unpublished decisions are not precedential, but they may be cited for their persuasive value. 10th Cir. R. 32.1(A).

chain of inferences. Moreover, when an alleged harm is not “certainly impending,” plaintiffs “cannot manufacture standing” under the guise of protecting against a purported prospective injury. Id. at 416.

Plaintiffs advance a plethora of alleged injuries to support their claims for damages and injunctive relief. They claim monetary damages for facing an “increased risk of fraud and identity theft,” “diminution in the value of [their] PII,” “time and expense related to monitoring . . . financial accounts,” “fear and anxiety due to increased risk [of harm],” and “lost value of personal information.” Dkt. # 21, at 6–7. They also request injunctive relief “as is necessary to protect the interests” of representative plaintiffs and the putative class.³ Id. at 36. Since the claims for injunctive relief are also predicated on finding plaintiffs indeed face an imminent risk of future identity theft or fraud, the Court addresses this alleged injury first.

While the Tenth Circuit has yet to consider this issue, many circuits have now assessed whether plaintiffs have standing when they receive notice that their data may have been subject to a data breach, but have not faced actual harm. See, e.g., Clemens, 48 F.4th at 152; McMorris v. Carlos Lopez & Assocs., 995 F.3d 295, 302 (2d Cir. 2021); Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1339 (11th Cir. 2021); In re Zappos.com, Inc., 888 F.3d 1020, 1024, 1027 (9th Cir. 2018); In re SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017); Beck v. McDonald, 848 F.3d 262, 273–75 (4th Cir. 2017); Attias v. Carefirst, Inc., 865 F.3d 620, 626 (D.C. Cir. 2017);

³ Plaintiffs request this Court to issue an order that would prohibit defendant from engaging in the wrongful and unlawful acts described in their complaint, require defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, require defendant to delete and purge the PII they do have, implement and maintain a security program, create firewalls, and engage third-party security auditors to perform a review of data. Dkt. # 21, at 36.

Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 692–94 (7th Cir. 2015); Katz v. Pershing, LLC, 672 F.3d 64, 79–80 (1st Cir. 2012). These courts have relied on a variety of non-dispositive factors to determine whether an alleged future risk of identity theft is imminent, including but not limited to, ascertaining (1) whether the data breach was intentionally targeted, (2) whether the data was misused, and (3) whether the data accessed was of a particularly sensitive nature. See Clemens, 48 F.4th at 153–54; McMorris, 995 F.3d at 301–03.

The Court finds, based on the above factors, that representative plaintiffs and the putative class have not established standing based on an increased and imminent risk of identity theft, fraud, or misuse. As to the first factor, it is unclear based on the complaint whether plaintiffs have sufficiently alleged that the attack was targeted. McMorris, 995 F.3d at 301 (“where plaintiffs demonstrate that a malicious third party intentionally targeted a defendant's system and stole plaintiffs’ data stored on that system, courts have been more willing to find . . . sufficient likelihood of future identity theft or fraud”); Reilly v. Ceridian Corp., 664 F.3d 38, 40, 44 (3d Cir. 2011) (finding no standing when it was “not known whether the hacker read, copied, or understood the data” on company servers and “no evidence that the intrusion was intentional or malicious”); cf. Cooper v. Bonobos, Inc., No. 21-CV-854, 2022 WL 170622, at *3 (S.D.N.Y. Jan. 19, 2022) (“data was stolen by a known ‘threat actor’ Shiny Hunters”); Clemens, 48 F.4th at 150 (finding that the data breach was intentional when a “hacking group known as CLOP accessed [company] servers through a phishing attack ...exfiltrat[ed] the data, installed malware to encrypt the data . . . held the decryption tools for ransom, threatening to release the information if [the company] did not pay the ransom”). Plaintiffs allege only that “certain client records were accessible to unauthorized parties

on the internet and that [d]efendant’s investigation ‘determined that there had been unauthorized access to Wing’s systems.’” Dkt. # 21, at 13 (cleaned up). Plaintiffs do not allege that a specific third party actor stole information, or that a known third party targeted Wing’s data server(s).⁴ Cf. Blood v. Labette Cnty. Med. Ctr., No. 22-cv-4036, 2022 WL 11745549, at *5 n.4 (D. Kan. October 20, 2022) (finding no injury when plaintiffs stated data was “removed from defendant’s system” but had not alleged their own sensitive information was “*actually* stolen”).

Assuming, *arguendo*, that the data breach was the result of a targeted attack, plaintiffs still fail to demonstrate that their data was misused. While some circuits have found that misuse by a third-party, while sufficient, is not necessary on its own to establish imminence, the majority of courts, including district courts in this circuit, have concluded that plaintiffs must allege actual misuse of to demonstrate they face an imminent risk of fraud. Clemens, 48 F.4th at 154 (noting that the Seventh Circuit has found that “misuse is not necessarily required”); but see C.C. v. Med-Data Inc., No. 21-2301, 2022 WL 970862, at *4 (D. Kan. Mar. 31, 2022) (“the Tenth Circuit . . . would follow the line of cases where [the] outcome depends on whether plaintiffs have alleged misuse of their data”); Legg, 574 F. Supp. 3d at 990 (“where no allegations of misuse are present, circuit courts have generally declined to find standing”); McCombs v. Delta Grp. Elecs., Inc., No. 22-CV-00662, 2023 WL 3934666, at *3 (D.N.M. June 9, 2023) (“Some circuit courts have concluded that data breach victims have sustained an injury in fact, but in nearly all instances, the allegations included the actual misuse of the data accessed.”). Representative plaintiffs’ closest allegations that misuse of their data occurred are the attempted charge to Stoichev’s Best Buy card and his increased receipt

⁴ Wing reported that “client records [relating to one Wing server] appeared to have been exposed to an unaffiliated third-party website.” Dkt. #34-1, at 5.

of spam phone calls. Dkt. # 21, at 6. Crucially, however, Stoichev fails to allege that he provided the information from his Best Buy card to Wing.⁵ In fact, Stoichev never alleges that he provided his phone number to Wing, nor that he was even a customer of Wing; he alleges that Wing received “highly sensitive personal and financial information” from him “as a consumer”. Dkt. # 21, at 4–5. Plaintiffs vaguely assert that Wing received “highly sensitive PII,” but do not allege specific facts about the nature of the information they provided to Wing. Dkt. # 21, at 2. It is therefore impracticable for the Court to conclude that these events alleged by Stoichev verify that data was misused in the breach. That no subsequent attempted instances of actual fraud have been made during the course of pleadings only bolsters this conclusion. In re Zappos.com, 108 F.Supp.3d 949, 958 (D. Nev. 2015) (“[T]he passage of time without a single report from [p]laintiffs that they in fact suffered the harm they fear must mean something.”)

Because plaintiffs have not alleged facts regarding the specific information they purportedly provided to Wing, the third factor— assessing the sensitive nature involved in the breach—does not tend to show that plaintiffs have standing. While the data breach did indeed expose highly sensitive PII, including social security numbers, driver license numbers, health insurance information, and financial account information, named plaintiffs do not allege *their* specific information nor those of the putative class, were released in the data breach. The Court concedes that the information

⁵ Stoichev asserts that he has “seen a marked increase in spam phone calls” but does not allege a particular quantity or attribute an increase in calls to the specific date of the data breach. Cf. Blood, 2022 WL 11745549, at *2 (finding injury in fact where plaintiff had alleged to receive between 10–15 spam calls per day since the specific month of the breach, among other harms such as unauthorized bank charges, IRS issues, and overdraft fees). Moreover, “courts have generally rejected the theory that unsolicited calls or emails constitute an injury in fact.” Cooper, 2022 WL 170622, at *5. This not only cuts against the misuse factor, but also Article III’s requirements of concreteness and traceability.

exposed in the breach would cut in plaintiffs favor had they affirmed that they provided that same sensitive information to Wing, but plaintiffs do not. Nor do representative plaintiffs establish that a relationship existed between Wing and clients that necessitated sharing specific sensitive information.⁶ See Clemens, 48 F.4th at 150 (plaintiff had provided her address, social security number, bank information, insurance, and passport as a condition of her employment with defendant); Attias, 865 F.3d at 622–23 (“customers purchased [defendant’s] insurance policies” and had to provide “their names, birthdates, email addresses, social security numbers, and credit card information”); In re SuperValu, Inc., 870 F.3d at 771–72 (grocery store customers had provided payment card information, which hackers stole). Even if Stoichev had alleged he gave his Best Buy card information or phone number to Wing, the sensitivity of that information does not rise to the high level of sensitivity contemplated in like cases. See McMorris, 995 F.3d at 302 (noting that “high-risk information” included “Social Security numbers and dates of birth”). If the Court were to conclude that named plaintiffs, based on the facts alleged here, faced an imminent risk of identity fraud or theft, then any individual who receives a notification of a company-wide data breach would have standing to sue. This notion contravenes TransUnion and data breach doctrine amongst the circuits.

The Court therefore finds that plaintiffs have not sufficiently alleged an injury based on an imminent risk of identity theft or fraud to support their claims for damages or injunctive relief. As to their allegations of *actual* identity theft in the form of “an attempted Best Buy transaction in another state and the receipt of multiple phone calls from loan companies,” the Court finds these

⁶ Plaintiffs assert only that “[c]lients are required to provide their sensitive personal information, including non-public financial information, to Wing as a condition of doing business.” Dkt. # 21, at 2.

stated injuries are not fairly traceable to the defendant. Dkt. # 29, at 13. Accepting these allegations as true, and even assuming these alleged harms are indeed concrete injuries in fact that are redressable by this Court, plaintiffs must demonstrate that an injury is “fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court” to withstand Article III’s standing requirements. Lujan, 504 U.S. at 560 (cleaned up); Safe Streets All. v. Hickenlooper, 859 F.3d 865, 878 (10th Cir. 2017). “[A]t the motion to dismiss stage, a plaintiff can satisfy the ‘fairly traceable’ requirement by advancing allegations which, if proven, allow for the conclusion that the challenged conduct is a ‘but for’ cause of the injury.” Santa Fe All. for Pub. Health & Safety v. City of Santa Fe, New Mexico, 993 F.3d 802, 814 (10th Cir. 2021), cert. denied sub nom., 142 S. Ct. 1228 (2022) (citations omitted). By failing to advance facts that they provided phone numbers, financial account numbers, or credit card information to Wing in the first place, plaintiffs cannot plausibly suggest Wing exposed that same data.

Because representative plaintiffs advance other injuries in support of their damages claim, the Court’s inquiry into standing does not terminate here. Plaintiffs’ remaining actual injuries—lost time “dealing with consequences,” “fear and anxiety,” and diminution in the value of their PII—nevertheless fail concreteness as required by Article III. Dkt. # 21, at 5. Plaintiffs may not invent harms to construct standing. See Clapper, 568 U.S. at 416. Since there exists no imminent threat of future harm, plaintiffs’ efforts to mitigate fraud in the form of lost time monitoring accounts “cannot create a concrete injury.” Legg, 574 F. Supp. 3d at 994 (citing In re SuperValu, Inc., 870 F.3d at 769 (“Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury.”)). This

reasoning holds for plaintiffs' allegations of heightened fear and anxiety as well.⁷ Clemens, 48 F.4th at 156 (finding a concrete injury only when an imminent risk of future identity theft existed and "the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services"). Since plaintiffs did not choose to enroll in Wing's complimentary credit monitoring services, have not alleged expenses incurred to protect their credit, and have not alleged that they changed their credit card or bank account numbers, asking this Court to conclude that they suffer concrete injuries resulting from this present fear of fraud alone is presumptuous. Cf. id. at 151 (finding concrete injuries when plaintiff enrolled in the complimentary credit monitoring, purchased \$40 credit protection services, transferred bank accounts, and paid for therapy). Finally, plaintiffs cannot allege that they have personally experienced a diminution in the value of their PII, since they do not allege facts suggesting that it has decreased in value or that plaintiffs were attempting to market their PII.⁸ Legg, 574 F. Supp. 3d at 994 ("Assuming personal identifying information has a monetary value, [p]laintiff fails to allege that he attempted to sell his personal information and was forced to accept a decreased price."); Cooper, 2022 WL 170622, at *5 (Plaintiff "does not plausibly allege that he intended to sell his personal information to someone else. Nor, in any event, does he plausibly allege

⁷ Fear and anxiety may be "sufficiently analogous to the tort of intentional infliction of emotional distress" (IIED) to satisfy concreteness. Clemens, F.4th 146 at 155. Without facing an imminent risk of identity theft, however, the distress of plaintiffs must manifest to that standard as required to establish IIED. In Oklahoma, IIED requires (1) that the defendant acted intentionally or recklessly; (2) that the defendant's conduct was extreme and outrageous; (3) that plaintiff actually experienced emotional distress; and (4) that the emotional distress was severe. Ishmael v. Andrew, 137 P.3d 1271, 1277 (Okla. Civ. App. 2006).

⁸ Plaintiffs generally allege that "personal information can be sold at a price ranging from \$40 to \$200." Dkt. # 21, at 18.

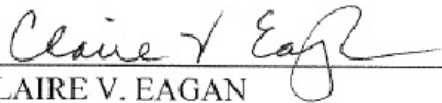
that someone else would have bought it as a stand-alone product”) (cleaned up); cf. Svenson v. Google Inc., No. 13-CV-04080, 2016 WL 8943301, at *7 (N.D. Cal. Dec. 21, 2016) (evaluating diminution in value of PII when plaintiff relied on specific prices at which their categories of PII were estimated to be reduced in value). Representative plaintiffs’ alleged facts have not manifested into concrete harms sufficient to confer standing.⁹ The Court therefore need not reach arguments pertaining to defendant’s motion to dismiss under Rule 12(b)(6).

⁹ Plaintiffs allege violations of the Health Insurance Portability and Accountability Act (HIPAA), the Federal Trade Commission Act, and the Oklahoma Consumer Protection Act, but cannot plead facts supporting private rights of action under any of these statutes. With respect to HIPAA, plaintiffs have not alleged facts substantiating that Wing, a tax services provider, would be a HIPAA-covered entity, nor that representative plaintiffs provided health information to Wing. Moreover, HIPAA does not create a statutory right of action. Wilkerson v. Shinseki, 606 F.3d 1256, 1267 n.4 (10th Cir. 2010); Med-Data Inc., 2022 WL 970862, at *6. Neither does the Federal Trade Commission Act. Drake v. Sometime Spouse, LLC, 784 F. App’x 602, 604 (10th Cir. 2019).

As to the Oklahoma Consumer Protection Act, it requires, among its four elements, that plaintiffs demonstrate they, as consumers, suffered an injury in fact. Hampton v. Gen. Motors, LLC, 631 F. Supp. 3d 1041, 1049–50 (E.D. Okla. 2022) (“To succeed in a private right of action under the OCPA, a plaintiff must establish: (1) that the defendant engaged in an ‘unlawful practice’; (2) that the challenged practice occurred in the course of defendant’s business; (3) that the plaintiff, as a consumer, suffered an injury in fact; and (4) that the challenged practice caused the plaintiff’s injury.”) Based on the aforementioned reasons, plaintiffs failed to allege sufficient facts supporting that they suffered an injury, and at any rate, cannot demonstrate defendant caused that injury. Plaintiffs therefore cannot assert a valid statutory right of action against Wing under the OCPA.

IT IS THEREFORE ORDERED that defendant's motion to dismiss (Dkt. # 25) is **granted** as to Rule 12(b)(1), and **moot** as to Rule 12(b)(6). A separate judgment of dismissal is entered herewith.

DATED this 19th day of September, 2023.



CLAIRE V. EAGAN
UNITED STATES DISTRICT JUDGE